p–ISSN: 2723 - 6609 e-ISSN: 2745-5254
Vol. 4, No. 11 November 2023 http://jist.publikasiindonesia.id/

IMPLEMENTATION OF NEXT-GENERATION FIREWALLS TO PROTECT APPLICATIONS FROM MALWARE ATTACKS

Herika Andini Putri[1]*, Nazel Djibran[2], Rohmat Tulloh[3]
PT Datacomm Diangraha Jakarta, Indonesia[1,3], Telkom University Bandung, Indonesia[2]
Email : herikas@student.telkomuniversity.ac.id[1]*, nazel.djibran@datacomm.co.id[2], rohmattulloh.rmt@gmail.com[3]

*Correspondence

ABSTRACT

Keywords: cybercrime; next-generation firewall; malware; Palo Alto.

Based on the rapid development of technology that has a positive and negative impact; one of the negative impacts is the leakage of data, called cybercrime. To overcome this, in this study, the design of the next-generation firewall (NGFW) protects technology and information systems from threats and malware attacks on technology and information systems. In this study, the Palo Alto firewall is implemented by configuring the firewall and testing the attack using malware. This test's results aim to prevent data loss, material loss, and paralysing of public services. Moreover, it is efficient and effective in scanning for variations of attacks without affecting network performance. The results' implications are expected to solve the problems faced perfectly. NGFW takes precautions by blocking malware access to its network traffic

Introduction

Along with the rapid development of technology and ongoing innovation and research, of course, there is a positive side, such as ease of communication and data exchange, and a negative side is the existence of cybercrime, namely attacks and data theft. This attracts public attention because attacks and data theft become increasingly high with sophisticated models as technology advances. One form of cybercrime is a zero-day attack, a high-potential threat because it exploits unknown vulnerabilities (Nugraha et al., 2022).

The negative impact of technological developments can result in losses, especially about essential information data that is only permitted to be known by certain people within a company. The most significant data leak case in the world, based on the CSO report, is the Yahoo data leak in August 2013, where around 3 billion accounts on their services were leaked (Kirana & Khalisah, 2022), so data security is a top priority to pay attention to from damage or misuse from unauthorised parties. Responsible.

One step that can be used to prevent data or information theft in a network is firewall technology (Purnomo et al., 2021). The function of a firewall is to protect the network from dangerous traffic. The firewall can be in the form of hardware or software. If illustrated, a firewall can be described as a gate. So when we send a packet from the internet, before it is sent to the user, the firewall will filter it and decide whether it is accepted or rejected.

Doi: *10.59141/jist.v4i11.797*

A firewall is a system that can apply access control policies to network traffic, which can help protect against network traffic attacks and other attacks and filter network traffic entering the network. Implementing a firewall on computer devices is essential to avoid the theft of confidential data. It is essential to implement a firewall on the network to protect against the threat of attacks. The primary performance of a firewall is that it can detect legitimate network traffic. So that access can be given to the system by passing through the firewall to be restricted. Restricting access to the local network prevents networks from being registered with the system. Restrictions are carried out by setting rules or policies in the firewall configuration. One type of firewall often discussed is the Next Generation Firewall (NGFW). Next-Generation Firewall is a firewall that can detect and block dangerous attacks. NGFW capabilities provide high protection and security and can implement security at the protocol, port and application levels.

Next-generation firewalls are part of the third generation of firewalls (Purnomo et al., 2021); the most apparent difference between the two is the ability of next-generation firewalls to filter each traffic based on application. Following-generation firewall users can use allowlists or signature-based IPS to differentiate between safe and unsafe applications.

Based on the phenomenon in the case above, namely, the vulnerability of data theft and data leaks, I have raised the title about implementing the next-generation firewall and how it works to defend against malware attacks. Because the next-generation firewall has more complex features in defending against malware, I used the next-generation firewall in this research.

In this research, I chose to secure the system with a next-generation firewall compared to a traditional firewall because traditional firewalls cannot block malware (Raharjo, 2022). This research will implement the exact implementation: web filters, antivirus, IPS and DDoS. However, apart from implementation, my research will test the resilience of next-generation firewalls against malware attacks (Pradipta, 2017).

Testing resistance to malware attacks on next-generation firewalls in this research uses ransomware, Wanna Cry and other malware. This research uses WannaCry because, according to the Palo Alto Unit 42 ransomware threat report, it is stated that the ransomware trend continues to increase. If you look at the report in 2022, ransomware cases will increase by 144% from the previous year and an 85% increase in the number of victims (Wibowo, 2023).

Wannacry has occurred since May 2017 and has paralysed over 200,000 computers in more than 150 countries (Syafira, 2020), with estimated total losses ranging from hundreds of millions to billions of US dollars. Wanna Cry works by encrypting all documents owned by the victim so that the victim cannot access these documents and also requires ransom from the victim to access the documents he owns. The target of this Final Project is expected to increase the defence of a firewall from malware attacks and help detect and prevent malware attacks early.

Research Methods

This research implements and tests the Next Generation Firewall's resistance to malware attacks.

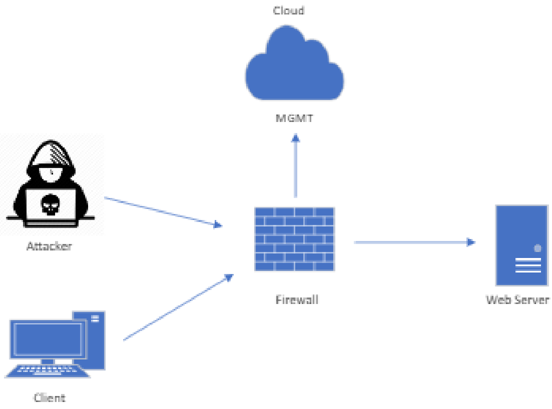


Figure 1 Design Topology

Based on Figure 1, it can be seen that the attacker carries out firewall resistance testing by sending malware files to the web server in zip form. After that, when the client accesses the web server, the attacker changes the malware file into an unzipped file so that when the client accesses the web server and opens the file, the malware will automatically enter the client, and because the web server passes through the firewall, the malware traffic log will be detected by the firewall.

The testing phase was carried out to see the resilience of the next-generation firewall and whether the system created was as expected. For this reason, a testing method, which is a measure or parameter, is needed to conclude that the system created is running according to its objectives. Some of the tests carried out include (Ratnawati, 2018):

1. Antivirus testing is carried out by trying to download malware such as Eicar, Ransomware and Trojans to see whether NGFW can block it.
2. Web filter testing is carried out by trying to access websites by entering the blocking category in the web filter to see whether the web filter is to see whether NGFW can prevent users from accessing websites that fall into the blocked category.

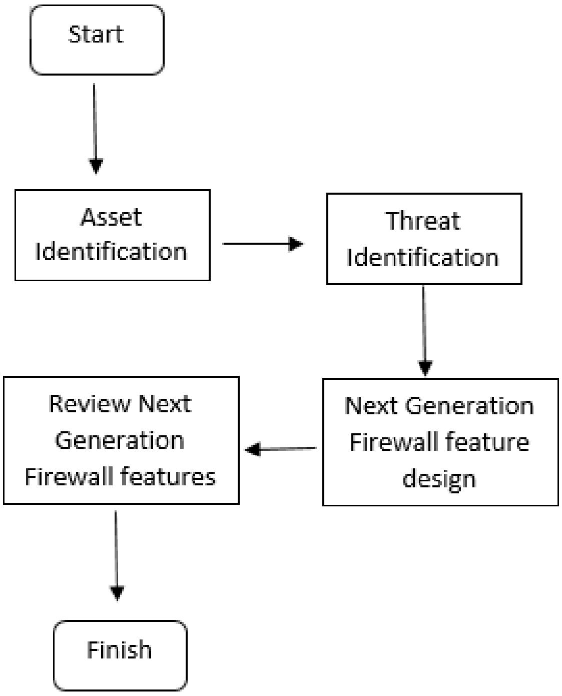

Start
Asset Identification
Threat Identification
Next Generation Firewall feature design
Review Next Generation Firewall features
Finish

Figure 2 Steps to Design the NGFW Basic Configuration

Figure 2 explains the steps for implementing the next-generation firewall, where the implementation will be carried out according to what is required, and where the firewall configuration will be carried out. The rule policy will be created according to the set (Zakir, 2015). The policy rules that will be created include antivirus and URL filtering. Some security features will be implemented, including the Intrusion Prevention System (IPS), network-based antivirus, and web filters. The first security feature is the Intrusion Prevention System (IPS), which scans and blocks activities considered suspicious and dangerous on networked computers, such as activities that exploit operating system weaknesses to find backdoors. The second security feature is a network-based antivirus that scans for viruses by scanning all network connections passing through Next-Generation devices (Siahaan, 2021).

In testing the resilience of this next-generation firewall, several scenarios will be tested to determine the reliability, efficiency and availability of the system being tested. The following are several scenarios in this research:

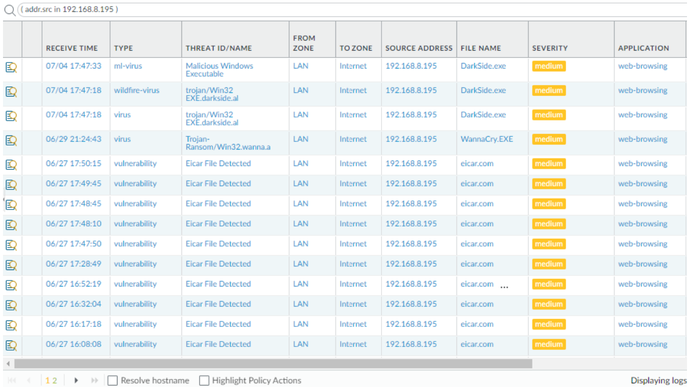
1. The testing system uses Eicar malware, Ransomware and then, finally, a Trojan
2. This test will be carried out by sending malware files to the web server so that when the client downloads the file, it will be detected in the firewall log.
3. Traffic log analysis on the firewall is used to determine whether the malware is detected on the firewall or not, and after the malware is detected, the firewall will then decide whether the malware file will be allowed or dropped according to the rule policy created.

4. Apart from using malware, web filtering tests will also be carried out by blocking dangerous websites so that they will be automatically blocked when someone opens the website.

Apart from malware testing, there is also zero-day malware testing, where the test uses unknown or new types of malware.

Results and Discussion

In this section, we will explain how the resilience of a firewall to block malware access has been tested. To test the resilience of the NGFW against malware, you need to create a web server that passes network traffic that is protected by the NGFW feature, where initially, the web server will be provided by the attacker with a malware file in the form of a zip, as you know, zip files will not be detected by firewalls (Sudarmadi & Runturambi, 2019). When the malware zip file is on the web server, the attacker will unzip the file so that when the client tries to access the file, it will be detected by the NGFW that the file being accessed is a malware file so that the file will be immediately blocked by the NGFW and log traffic. It will appear on the firewall.



(addr.src in 192.168.8.195)

RECEIVE TIME	TYPE	THREAT ID/NAME	FROM ZONE	TO ZONE	SOURCE ADDRESS	FILE NAME	SEVERITY	APPLICATION
07/04 17:47:33	ml-virus	Malicious Windows Executable	LAN	Internet	192.168.8.195	DarkSide.exe	medium	web-browsing
07/04 17:47:18	wildfire-virus	trojan/Win32 EXE.darkside.al	LAN	Internet	192.168.8.195	DarkSide.exe	medium	web-browsing
07/04 17:47:18	virus	trojan/Win32 EXE.darkside.al	LAN	Internet	192.168.8.195	DarkSide.exe	medium	web-browsing
06/29 21:24:43	virus	Trojan-Ransom/Win32.wanna.a	LAN	Internet	192.168.8.195	WannaCry.EXE	medium	web-browsing
06/27 17:50:15	vulnerability	Eicar File Detected	LAN	Internet	192.168.8.195	eicar.com	medium	web-browsing
06/27 17:49:45	vulnerability	Eicar File Detected	LAN	Internet	192.168.8.195	eicar.com	medium	web-browsing
06/27 17:48:45	vulnerability	Eicar File Detected	LAN	Internet	192.168.8.195	eicar.com	medium	web-browsing
06/27 17:48:10	vulnerability	Eicar File Detected	LAN	Internet	192.168.8.195	eicar.com	medium	web-browsing
06/27 17:47:50	vulnerability	Eicar File Detected	LAN	Internet	192.168.8.195	eicar.com	medium	web-browsing
06/27 17:28:49	vulnerability	Eicar File Detected	LAN	Internet	192.168.8.195	eicar.com	medium	web-browsing
06/27 16:52:19	vulnerability	Eicar File Detected	LAN	Internet	192.168.8.195	eicar.com ...	medium	web-browsing
06/27 16:32:04	vulnerability	Eicar File Detected	LAN	Internet	192.168.8.195	eicar.com	medium	web-browsing
06/27 16:17:18	vulnerability	Eicar File Detected	LAN	Internet	192.168.8.195	eicar.com	medium	web-browsing
06/27 16:08:08	vulnerability	Eicar File Detected	LAN	Internet	192.168.8.195	eicar.com	medium	web-browsing

A. Results of a Phishing Attack

The results of the phishing test with NGFW, NGFW rejected files containing viruses sent from attackers, NGFW rejected files sent to the web server because NGFW detected a virus-like pattern in the attachment (eicar.com), and after matching it with an antispam database owned by NGFW, then NGFW concludes that the attachment contains a virus and the file is rejected (Abidin, 2021).

B. Results of a Ransomware Attack

The results of the WannaCry ransomware attack test with NGFW, because NGFW detected a pattern resembling ransomware and after matching it with the antivirus database owned by NGFW, NGFW concluded that the file contained malware and the file was dropped (Liang & Kim, 2022).

C. Result of a Trojan Attack

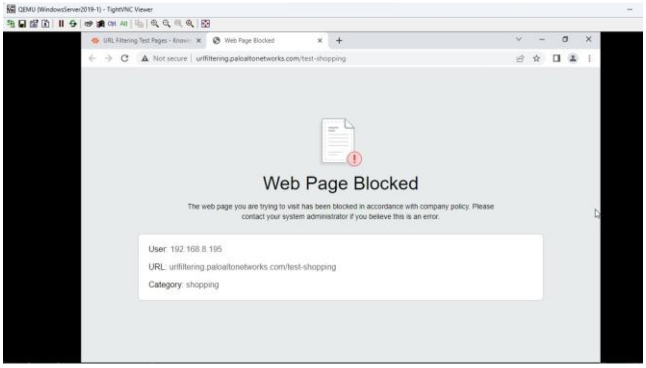
The results of the trojan test with NGFW few rejected files containing viruses sent from attackers; NGFW rejects files sent to the file server because NGFW detects a virus-like pattern in the attachment. After matching it with the antispam database owned by NGFW, NGFW concludes that the attachment contains a virus, and the file is rejected.

Table I.
Recapitulation Of Attack Test Results

No	Attack Type	Attack Method	Attack Target	Response NGFW
1	Phishing	Send Spam Mail with Virus	Website Server	Drop
2	Ransomware	Send Spam Mail with Virus	Website Server	Drop
4	Trojan	Send Spam Mail with Virus	Website Server	Drop

D. Results from Web Filtering Testing

Web filtering testing is implemented by blocking dangerous sites or websites such as gambling websites, online games and so on so that when a user opens a dangerous website, even though the device connectivity can ping, which proves that the network can be accessed, the dangerous website cannot be accessed (Tosepu, 2018).


QEMU (WindowsServer2019-1) - TightVNC Viewer
URL Filtering Test Pages - Knowl
Web Page Blocked
Not secure
urlfiltering.paloaltonetworks.com/test-shopping

Web Page Blocked

The web page you are trying to visit has been blocked in accordance with company policy. Please contact your system administrator if you believe this is an error.

User: 192.168.8.195

URL: urlfiltering.paloaltonetworks.com/test-shopping

Category: shopping

Network performance testing can be done by pinging the detik.com site. It can be seen that the average latency that occurs is 61 ms, and when internet traffic is passed to the NGFW, the average latency is 48 ms. To find out the speed of opening a website, a test was carried out by opening the detik.com website, where the results obtained were an increase in Internet network usage to access the detik.com website is 3.25 seconds, meanwhile, when internet traffic is passed to the NGFW the time to be able to access the detik.com website is 1.31 seconds.

Table II tests it by comparing the network performance speed between the network with NGFW and the network without NGFW. By using the Next-Generation Firewall that has been implemented, many aspects can be improved. The results of this research are shown in Table II, which shows a perfect improvement, where a network that initially did not have a security system to protect technology and information systems now has a Next-Generation Firewall.

Table 2
Recapitulation Of Attack Test Results

Measurement	NGFW no-distribution	Distributed NGFW	Change
Average Latency	61 ms	48 ms	Increased latency performance by 27%
Average website access time	3.25 seconds	1.31 seconds	Increased average website access time by 59.68%
Measurement	Network Layer (L3)	Application Layer (L7)	100%
NGFW security features	Nothing	IPS. Antivirus, Web Filter. WAF	100%

E. Results from wildfire testing

Wildfire testing is used to see how Next Generation Firewall protects an application from unknown or zero-day malware attacks. The role of the Next Generation Firewall here is that when there is a zero-day malware attack, Wildfire will detect the malware, and a log or traffic will be sent after 5 minutes of the attack because Wildfire reads the log when a message comes to Palo Alto. It can be said that Wildfire is the same as a sandbox (Novitasari, 2018).

The attack traffic log will be detected for 5 minutes due to the wildfire process itself; the wildfire feature will detect malware with a hash file so that the process is when an unknown file passes through the NGFW, then the NGFW will check and analyse whether the wildfire feature has seen it—The file or not. If the file has never been identified, then action will be taken by the provisions of Wild Fire itself; it will be adjusted to what the capacity of the file is and whether the file is trusted or not by the database on the NGFW so that after this has been done Wild Fire will decide whether the file is malware. Or not.

Wildfire testing is beneficial because, with the wildfire feature, network security is better protected from unknown malware attacks. As technology develops, malware develops in new forms and is more updated than previous malware.

Conclusion

After implementing and testing the NGFW, it can be concluded that the complete features available on the NGFW, such as Intrusion Prevention System (IPS), Antispam and mail, Threat Emulation, URL Filtering, and Application Control, can make the data communication network safer. It can be seen in the results of the tests that have been carried out, where the three attacks carried out in this final project (Ransomware, Trojan, phishing and web filtering) can be detected and can be driven by the NGFW because the NGFW can carry out inspections based on the content and behaviour of each data packet that passes through NGFW so that NGFW can block before the data packet enters the network. Apart from that, with the presence of NGFW, the speed of a network to access a website increases because, as in the data shown in Table II, the average latency on a network that passes NGFW traffic will be more negligible compared to the average latency value that does not pass NGFW traffic because the average latency value is smaller. The better the website access speed of a network.

Bibliography

Abidin, A. M. (2021). Pendidikan moral dan relevansinya dengan pendidikan Islam. *Jurnal Paris Langkis*, *2*(1), 57–67.

Kirana, P., & Khalisah, A. M. (2022). Implementasi Norma Hukum Terhadap Tindak Pidana Peretasan (Hacking) di Indonesia. *Jurist-Diction*, *5*(6).

Liang, J., & Kim, Y. (2022). Evolution of firewalls: Toward secure network using a next-generation firewall. *2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC)*, 752–759.

Novitasari, N. (2018). Pengaruh karakteristik gambut terdegradasi terhadap kebakaran lahan gambut (Studi kasus lahan gambut PLG Blok A di Kalimantan Tengah). *Prosiding Seminar Nasional Lingkungan Lahan Basah*, *3*(2).

Nugraha, A. A., Lukitaningtyas, Y. K. R. D., Ridho, A., Wulansari, H., & Al Romadhona, R. A. (2022). Cybercrime, Pancasila, and Society: Various Challenges in the Era of the Industrial Revolution 4.0. *Indonesian Journal of Pancasila and Global Constitutionalism*, *1*(2).

Pradipta, Y. W. (2017). Implementasi Intrusion Prevention System (IPS) Menggunakan Snort Dan IP Tables Berbasis Linux. *Jurnal Manajemen Informatika*, *7*(1), 21–28.

Purnomo, R. F., Purbo, O. W., & Aziz, R. Z. A. (2021). *Firebase: Membangun Aplikasi Berbasis Android*. Penerbit Andi.

Raharjo, B. (2022). Audit Sistem Informasi Akuntansi. *Penerbit Yayasan Prima Agus Teknik*, 1–204.

Ratnawati, F. (2018). Implementasi Algoritma Naive Bayes Terhadap Analisis Sentimen Opini Film Pada Twitter. *INOVTEK Polbeng-Seri Informatika*, *3*(1), 50–59.

Siahaan, E. S. P. (2021). *Perancangan Dan Implementasi Virtual Private Network Dengan Mikrotik*. Prodi Teknik Informatika.

Sudarmadi, D. A., & Runturambi, A. J. S. (2019). Strategi Badan Siber Dan Sandi Negara (Bssn) Dalam Menghadapi Ancaman Siber Di Indonesia. *Jurnal Kajian Stratejik Ketahanan Nasional*, *2*(2), 157–178.

SYAFIRA, A. (2020). *Upaya Sekuritisasi Pemerintah Inggris Dalam Kebijakan Kejahatan Cyber Wannacry Tahun 2017*.

Tosepu, Y. A. (2018). *Media Baru dalam Komunikasi Politik (Komunikasi Politik I Dunia Virtual)*. Jakad Media Publishing.

Wibowo, A. (2023). Internet of Things (IoT) dalam Ekonomi dan Bisnis Digital. *Penerbit Yayasan Prima Agus Teknik*, 1–94.

Zakir, S. (2015). Pemanfaatan Sms Gateway Untuk Sistem Keamanan Desain Dan Implementasi Networking Security Memanfaatkan Security Configuration Wizard (Scw). *Jurnal Processor*, *10*(2), 491–498.